Toward a secure group communication: state of the art and perspectives

Vers une communication de groupe sécurisée : état de l'art et perspectives

Ghassan Chaddoud, Isabelle Chrisment et André Schaff

Novembre 1999

Vers une communication de groupe sécurisée : état de l'art et perspectives

Ghassan Chaddoud, Isabelle Chrisment et André Schaff

Projet RESEDAS

Rapport de recherche
Novembre 1999
19 pages

Résumé : Avec l'émergence de nouvelles applications coopératives multimédia, la communication de groupe est clairement devenue un concept important dans l'architecture réseau. La transmission multipoints apparaît comme le moyen le plus efficace d'envoyer des données à un groupe spécifique composé de plusieurs membres. De plus, l'intérêt croissant dans la communication réseau à travers l'utilisation de l'Internet a rendu nécessaire des services comme l'authentification, l'intégrité et la confidentialité pour transporter des données de manière sûre. Dans ce papier nous présentons un état de l'art relatif à la communication de groupe sécurisée. Nous décrivons les différentes approches existantes pour distribuer et gérer les clés dans un groupe. Nous développons comment la sécurité dans un groupe est traitée au niveau IP. Nous montrons qu'actuellement aucun modèle de sécurité ne satisfait complément les besoins requis pour une communication de groupe.

Mots-clé : Sécurité, Multipoint, Authentification, Protocole Internet, Communication de Groupe, IPSec.

(Abstract: pto)

LORIA
Campus scientifique
BP 23, 54506 VANDŒUVRE LÈS NANCY (France)
Téléphone : 03 83 59 30 30 - International : +33 3 3 83 59 30 30
Télécopie : 03 83 27 83 19 - International : +33 3 83 27 83 19

Toward a secure group communication: state of the art and perspectives

Abstract: With emerging of new cooperative applications, the group communication is clearly become a very important concept within the network architecture. The multicast transmission is appeared as the most efficient way to send some data to a specific group composed of several members. Moreover, the increasing interest in network communication through the using of the Internet made needed somes services such authentication, integrity and confidentiality to transport securely data. In this paper we present a survey about secure multicasting. We describe the different approaches to distribute and manage the keys within a group. We point out how the IP multicast security is dealt with. We show that presently no security model meets fully the requirements needed for group communication.

Key-words: Security, Multicast, Authentication, Internet Protocol, Group Communication, IPSec.

1 Introduction

L'évolution rapide des technologies vers des réseaux haut-débit, la vitesse de plus en plus rapide des processeurs ont favorisé le développement de nouvelles classes applications comme l'audio, la vidéo conférence et le tableau blanc partagé. Pour ces applications coopératives la communication de groupe est devenue un concept non seulement important mais nécessaire. La transmission multipoints apparaît comme le moyen le plus efficace pour envoyer des données vers plusieurs récepteurs en réduisant la bande passante utilisée.

De plus, l'utilisation croissante des réseaux comme l'Internet pour des communications privées ou commerciales accroît l'importance liée à la sensibilité des données et nécessite des services comme l'authentification, l'integrité et la confidentialité pour transporter les informations de façon sûre.

Beaucoup de recherches ont été effectuées pour protéger la communication point-à-point et des standards ont émergés ([Atkinson 98b, Harkins 98, Maughan 98],...). Ce n'est pas le cas pour la communication de groupe qui, pourtant, est plus complexe à sécuriser :

- le multicast présente plus d'opportunité pour l'interception du trafic ;
- si une attaque se produit alors un grand nombre de systèmes peuvent être affectés ;
- l'identité et l'adresse du groupe sont connues à large échelle ce qui aide les intrus à diriger leurs attaques ;
- Les attaquants peuvent remplacer des membres principaux (membres légitimes du groupe) par d'autres membres illégitimes.

La communication de groupe implique aussi des problèmes spécifiques qui peuvent influencer l'architecture et les modèles de sécurité [Canetti 98a]:

- `Passage à l'échelle.` La taille de groupe peut varier d'une dizaine de participants dans les petits groupes de discussion, à plusieurs centaines voire plusieurs milliers dans les conférences virtuelles sur l'Internet.
- `Caractéristiques des membres.` Les conditions matérielles (type de machines) ou d'infrastructures réseaux peuvent être hétérogènes entre les membres impliquant des besoins en communication différents.
- `Dynamicité.` La taille du groupe peut évoluer durant une session. Des membres peuvent ainsi joindre et quitter la session à n'importe quel instant. Tous les membres ne sont pas nécessairement actifs durant une session.
- `Contrôle du groupe.` Il n'y a pas toujours un système central bien informé de l'état des membres du groupe.
- `Durée de vie.` Le groupe peut exister de manière temporaire ou permanente.
- `Type de membres` (émetteur/récepteur). Cela dépend du modèle de groupe utilisé : soit le modèle 1-N où un seul membre peut envoyer un message et le modèle N-N où n'importe quel membre peut envoyer et recevoir des messages.

Dans ce papier nous nous intéressons à la confidentialité, à l'intégrité et à l'authentification des données échangées dans un groupe. Leur mise en œuvre reste problématique car elle nécessite la création et la distribution des clés aux membres du groupe, d'une manière sécurisée.

Le but de cet article est de réaliser un état de l'art sur la sécurité dans la communication de groupe, en mettant en évidence les problèmes posés et en décrivant et comparant les différentes approches proposées. La structure de ce papier est la suivante. La section 2 soulève les problèmes liés à la sécurité multicast, notamment celui d'extensibilité. Afin d'assurer les services de sécurité (confidentialité, intégrité et authentification), les membres d'un groupe doivent partager un ensemble de paramètres composant la GSA (Group Security Association en anglais) qui sera étudiée en 3^{eme} section.

Les principaux paramètres de la GSA sont les clés utilisées pour assurer la confidentialité et l'authentification. Les section 4 et 5 décrivent les différentes approches proposées pour la gestion des clés de confidentialité et d'authentification. Quant à la 6^{eme} section, elle décrira les travaux menés par l'IETF pour assurer les communications de groupe sur l'Internet.

2 Problématiques

La tâche fondamentale d'un protocole de sécurité multicast est de permettre seulement aux membres autorisés d'accéder au trafic du groupe. En général, les protocoles multicasts présentent deux problèmes qui limitent le passage à l'échelle ou l'extensibilité. Ces problèmes ont été résumés par [Mittra 97] sous les termes **1 affect n** et **1 does not equal n**.

- **1 affect n :** se produit lorsque une action chez un membre du groupe affecte tous les autres membres. Par exemple, dans le protocole DVMRP [Pusteri 99], l'ajout d'un système émetteur provoque la construction d'un nouvel arbre basé sur la source et tous les routeurs doivent alors mettre à jour l'état d'information du groupe.
- **1 does not equal n :** apparaît quand un protocole ne peut pas traiter avec tous les membres d'un groupe ; il doit prendre en compte les capacité de chacun. MITTRA [Mittra 97] cite les protocole de contrôle de flux quand il y a des récepteurs qui veulent augmenter le rythme de transmission et d'autres qui veulent le diminuer.

Les protocoles de gestion de clés multicasts rencontrent le problème de type **1 affect n** lors de l'ajout d'un nouveau membre au groupe et les deux types de problèmes lors de la suppression d'un membre.

Quand un nouveau membre se joint au groupe, l'entité responsable de la gestion de clés doit remplacer la clé du groupe K_{grp} (la clé commune entre les membres du groupe et utilisée pour chiffrer le communication multicast du groupe) par une autre $K_{grp}{}'$ afin d'empêcher un nouvel abonné au groupe d'accéder à l'ancien trafic. La clé actuelle K_{grp} du groupe est utilisée pour distribuer la nouvelle clé $K_{grp}{}'$. Un seul message contenant $K_{grp}{}'$ chiffré avec K_{grp} est diffusé à l'ensemble du groupe. Les membres du groupe qui reçoivent ce message remplacent K_{grp} par $K_{grp}{}'$. L'ajout d'un seul membre oblige donc tous les autres membres

à remplacer la clé du groupe. L'ajout d'**1** seule entité affecte les **n** (taille du groupe) autres entités.

Quand un membre quitte le groupe, l'entité responsable de la gestion de clés doit remplacer aussi la clé du groupe K_{grp} afin d'empêcher le membre supprimé d'accéder aux futures communications du groupe. Le gestionnaire de clé crée une nouvelle clé $K_{grp}{}'$ comme dans le cas précédent, mais cette fois il ne peut pas distribuer la nouvelle clé par un seul message multicast chiffré avec l'ancienne clé. Le membre supprimé pourrait déchiffrer ce message et avoir la nouvelle clé. Par conséquent, le gestionnaire de clé est obligé d'utiliser des tunnels sécurisés de communication pour communiquer $K_{grp}{}'$ à chaque membre individuellement. Les deux types de problèmes d'extensibilté se rencontrent : le premier est **1 does not equal n** car le gestionnaire communique la clé à un membre comme s'il était indépendant du groupe. Le deuxième est **1 affect n** car la suppression d'un seul membre oblige les n membres à remplacer la clé K_{grp} par une autre.

Lors de la mise à jour de la clé du groupe, d'autres problèmes d'extensibilité se manifestent sous forme de trous de sécurité dus à une communication asynchrone entre les différents membres :

- les membres récepteurs, qui n'arrivent pas à recevoir la nouvelle clé, ne peuvent plus être capables de déchiffrer les communications du groupe. De plus, ils risquent de recevoir des communications envoyées par des membres supprimés ;
- les membres émetteurs qui n'arrivent pas à recevoir la nouvelle clé, continuent de chiffrer les messages émis avec l'ancienne clé ; les autres membres ne sont plus capables de recevoir les messages du groupe. De plus, des membres supprimés peuvent être capables de déchiffrer les messages ; ce qui compromet la sécurité du groupe.

Le problème de synchronisation peut-être résolu en utilisant des protocoles de multicast fiables comme SRM [Floyd 95].

Après avoir parlé de la sécurité de groupe, nous détaillerons dans les sections 4 et 5 des solutions proposées pour l'établissement des clés, en particulier, de celles qui essayent de résoudre le problème d'extensibilité.

3 Gestion de sécurité d'un groupe

Un protocole de sécurité doit permettre aux entités autorisées de communiquer, d'une manière sécurisée, sur un réseau non assuré où des intrus peuvent lire, effacer ou modifier le trafic. Ceci est réalisé par la création d'une association de sécurité entre les entités autorisées par le biais de protocoles d'authentification et d'échanges de clés. L'association de sécurité ou SA (Security Association en anglais) peut être utilisée afin de réaliser des objectifs de sécurité comme l'authentification, l'intégrité et la confidentialité.

Dans le cas d'une communication point-à-point, la SA est gérée par les deux parties. Par contre, la SA de groupe ou GSA ne peut pas être gérée par toutes les parties participantes. La gestion de la SA de groupe signifie la gestion de la sécurité du groupe plus particulièrement le contrôle d'accès au groupe (*i.e.* au trafic multicast du groupe).

3.1 L'Association de Sécurité ou SA

L'association de sécurité SA (Security Association) définit un ensemble de paramètres (algorithmes et clés de chiffrement, algorithmes et clés d'authentifications, durée de vie de ces paramètres, ...) partagés entre les membres authorisés. Ces paramètres peuvent être utilisés pour assurer des services de sécurité tels que l'authentification, l'intégrité et la confidentialité.

L'architecture de sécurité IPsec [Atkinson 98b] définit les concepts de base de SA entre deux parties, *i.e.* SA unicast. Cette SA est négociable par le biais des algorithmes déjà définis comme ISAKMP/IKE [Maughan 98, Harkins 98]. Une SA unicast est un ensemble de données communes entre 2 entités communicant sur le réseau, qui sont connues d'elles seules et qui leur permettent d'avoir un "canal virtuel" de communication sécurisé. Cette protection peut aller de la simple authentification au chiffrement fort associé à l'authentification. Cette SA est unidirectionnelle, *i.e.* valable dans une seule direction. Deux entités communiquant utilisent deux SA, une dans chaque sens. Une SA unicast est identifiée par le triplet:

- l'adresse IP du destinataire ;
- le SPI (Security Parameter Index en anglais). C'est un numéro particulier que l'on peut fixer arbitrairement ;
- et un protocole (ex: AH [Atkinson 98a] pour l'authentification ou ESP [Atkinson 95] pour le chiffrement).

3.2 L'Association de Sécurité de groupe ou GSA

Dans le cas de communication multicast, l'association de sécurité GSA (Group Security Association) n'est pas négociable, *i.e.* les membres du groupe ne peuvent pas dialoguer entre eux pour créer une GSA car le nombre de participants est relativement important. Dans [Atkinson 98b, Hardjono 99b] il est proposé qu'une seule entité par exemple, le manager du groupe, puisse choisir une GSA (donc un seul SPI appelé GSPI) pour le trafic multicast du groupe. Puis, cette entité distribue cette GSA aux membres du groupe par le biais de tunnels sécurisés point-à-point. Tous les membres du groupe doivent utiliser le même GSPI lié à la GSA. Lors du renouvellement de la clé du groupe, un nouveau GSPI doit être choisi pour la GSA et une nouvelle clé du groupe doit être créée par une entité. Enfin, elle est distribuée aux membres du groupe.

Rappelons que pour une SA unicast, deux parties choisissent les paramètres de SA selon leur capacité cryptographique (e.g algorithmes d'authentification, algorithmes de cryptage,...). Dans le cas de GSA choisie par une entité, les besoins en algorithmes (des paramètres de sécurité) des membres du groupe, doivent être annoncés en avance par d'autres méthodes comme les protocoles multicasts de description de session. Deux types de GSA sont différenciés dans [Monga 99] :

1. Le premier pour le multicast 1-à-N dans les groupes avec un seul émetteur dans le groupe. Une GSA est identifiée par le triplet : l'adresse IP de l'émetteur, le GSPI et un protocole (ex. AH, ESP). Ce triplet est le mirroir du triplet (l'adresse IP du destinataire, SPI, protocole) identifiant une SA unicast.

2. Le deuxième pour le multicast N-à-N dans les groupes avec plusieurs émetteurs. Plusieurs couches (nombres d'émetteurs) de 1-à-N sont superposées pour les protocoles de routage multicast qui ne supportent que 1-à-N groupes de multicast, *i.e.* un arbre unidirectionnel de distribution. En fait, cette proposition n'est pas la bonne solution pour les groupes avec un grand nombre d'émetteur.

3.3 Contrôle d'accès au groupe

Dans la littérature, nous trouvons deux stratégies de gestion de la sécurité multicast : la gestion centralisée et la gestion décentralisée.

- La gestion centralisée est définie par le fait qu'une seule entité contrôle la sécurité du groupe [Harney 97a, Wallner 98, Wong 98]. HARNEY ET MUCKNHIRN [Harney 97a] utilisent une seule entité pour gérer le groupe, cette entité s'appelle le contrôleur du groupe, en abrégé CG. Le CG contrôle l'accès au groupe en distribuant les clés du groupe aux participants autorisés (*i.e.* qui ont une une permission certifiée par une autorité). Le trafic multicast diffusé par chaque participant arrive à tous les participants. Par contre, [Wallner 98, Wong 98] bénificient d'un arbre hiérarchique. Il permet aux participants ayant la même clé qui se trouve à la racine d'un sous-arbre de l'arbre hiérarchique, de communiquer entre eux, autrement dit les participants du groupe peuvent être divisés en sous-groupe. Mais, les données multicasts sont toujours contrôlées par le CG qui se trouve à la racine de l'arbre et qui gère le groupe.
- La deuxième stratégie consiste à décentraliser la gestion du groupe [Mittra 97, Hardjono 99a, Hardjono 99b] et à diviser le groupe du multicast en sous-groupes. Chaque sous-groupe, géré par un contrôleur local, possède sa propre clé. Les sous-groupes sont liés par l'intemédiaire des agents pour construire un groupe virtuel. Le rôle des agents intermédiaires est de traduire les données multicasts diffusées par un membre dans un sous-groupe à tous les membres du groupe virtuel.

En comparant ces deux stratégies, nous constatons que la deuxième stratégie représente une solution au problème d'extensibilité **1 affect n**. L'ajout et la suppression d'un membre affecte seulement le sous-groupe auquel il appartient. En conséquence, cette stratégie répond mieux au dynamisme du groupe, mais elle est moins efficace pour la diffusion des données car elle subit des opérations de déchiffrement/rechiffrement par les agents intermédiaires. Par contre, la première stratégie est plus efficace pour la diffusion car elle utilise une seule clé commune à tous les membres du groupe. Le problème de cette stratégie est la centralisation de la gestion du groupe : une seule entité contrôle le groupe. Si cette entité tombe en panne, le groupe devient sans contrôle, voire hors de fonctionnement.

Dans les deux sections suivantes, nous allons analyser et comparer des approches proposées pour la construction et la distribution des clés servant à chiffrer le trafic multicast.

4 Établissement et distribution des clés de groupe

Afin d'assurer la confidentialité aux communications de groupe, les membres du groupe partagent un secret appelé une clé du groupe ou clé multicast, k_grp en abrégé. Un message multicast envoyé par un membre du groupe et chiffré avec k_grp peut être reçu et déchiffré par tous les membres qui ont la même clé. L'entité responsable de cette clé est le manager ou le contrôleur dugroupe. Cette entité crée et distribue la clé, d'une manière sécurisée, aux différents membres du groupe.

Les approches utilisées pour l'établissement et la distribution de clés du groupe peuvent être classifiées, selon [Balenson 99], en cinq catégories :

1. approches basées sur la théorie d'information ;
2. approches hybrides ;
3. approches d'échange de clé de Diffie-Hellmann de groupe ;
4. approches SKDC (Single Key Distribution Center) qui sont linéaires avec la taille du groupe ;
5. approches hiérarchiques.

Les trois premières catégories correspondent à des méthodes théoriques et difficiles à implémenter. Tandis que les approches SKDC et hiérarchiques sont plus pragmatiques.

4.1 Approches de théorie d'information

Ces approches se basent sur la théorie d'information. La sécurité des clés de groupe est basée sur la notion d'entropie. Ainsi [Blundo 92] propose un schéma de distribution des clés pour les conférences dynamiques. Un fidèle serveur, un tiers et non pas un participant à la conférence, distribue des pièces d'informations privées et individuelles à un ensemble d'usagers. Ultérieurement, un sous-ensemble de ces usagers de taille donnée peut calculer une clé commune sécurisée. Chaque usager calcule la clé commune à partir des identités des autres usagers dans le sous-groupe et de sa propre pièce d'information.

Afin d'assurer la sécurité de la clé du groupe contre les coalitions des membres supprimés, les approches de théorie d'information exigent un espace de stockage exponentiel.

4.2 Approches hybrides

Ces approches sont au minimum linéaires par rapport à la taille du groupe. Elles réduisent l'espace de stockage en trouvant un compromis entres différentes stratégies de sécurité de théorie d'information. C'est le cas de [Fiat 93] qui permet à un site central de diffuser des transmissions sécurisées à un ensemble arbitraire d'usagers.

Soit un centre et un groupe d'usagers. Le centre fournit à chaque usager joignant le groupe un ensemble de clés. À un moment donné, le centre diffuse un message à un sous-ensemble privilégié d'usagers tel que les autres ne peuvent pas le déchiffrer. Chaque participant du sous-ensemble doit être capable de calculer la clé avec laquelle le message est chiffré.

4.3 Diffie-Hellmann de groupe

Ces approches se basent sur l'algorithme de Diffie-Hellman d'échange de clé entre deux parties [Schneier 97]. Nous pouvons citer comme exemple [Steiner 96, Burmester 97]. Chaque membre i du groupe contribue à la construction de la clé du groupe par un nombre aléatoire N_i. La clé du groupe est q^S mod p; où S est le produit des N_i ($i \in \{1...n\}$). Le protocole se base sur le calcul distribué du sous-ensemble $\{q^{\pi(S)}, S \subset \{N_1,...,N_n\}\}$ de $q^{N_1,...,N_{i-1},N_{i+1},...,N_n}$. Le membre M_i calcule facilement $((q^{N_1,...,N_{i-1},N_{i+1},...,N_n} mod p)^{N_i})$ mod p. Le nombre de messages échangés entre les différents membres, pour construire la clé du groupe, est de l'ordre n (*i.e.* O(n)). Ces approches offrent une fonctionnalité distribuée de calcul mais, elle souffrent d'un nombre linéaire important d'opérations à clés publiques qui sont très coûteuses.

4.4 Approches SKDC (Single Key Distribution Center)

Elle sont linéaires avec la taille du groupe, *i.e.* d'un point de vue algorithmique, elles sont extensibles linéairement avec le nombre de participants dans le groupe. C'est la cas, par exemple, de GKMP (Group Key Management Protocol) [Harney 97a, Harney 97b] et [Wallner 98]. Un SKDC, ou un centre de distribution de clés, est un participant du groupe, et non pas un tiers, qui coopère avec un autre participant pour créer la clé du groupe. L'approche SKDC utilise une technique d'échange à clé publique (e.g Diffie-Hellmann d'échange à clé publique [Schneier 97]) pour créer la clé du groupe et pour la distribuer aux autres participants. De ce fait, le nombre de messages émis à chaque retrait ou ajout d'un membre, et le nombre d'opérations de calcul effectuées par le manager du groupe est d'ordre n (n est la taille du groupe).

Malgré la compléxité linéaire, cette approche reste l'approche la plus simple pour les petits groupes.

4.5 Approches hiérarchiques

Ces approches sont extensibles logarithmiquement avec la taille du groupe. Nous pouvons distinguer deux types : les approches qui nécessitent des routeurs fidèles comme dans [Ballardie 96] et les approches qui n'exigent pas des nœuds intermédiaires fidèles. C'est le cas, par exemple, de la hiérarchie de clé logique LHK (Logical Key Hierarchy) [Wallner 98, Wong 98] et l'arbre OFT (One-way function Tree) [McGrew 98, Balenson 99]. Dans la suite nous parlerons de SMKM qui nécessite des nœuds intermédiaires puis nous détaillerons LHK et OFT.

4.5.1 SMKM [Ballardie 96]

SMKM (Scalable Multicast Key Distribution) exige des routeurs fidèles. Elle se base sur le protocole CBT (Core Based Tree) de multicast [Ballardie 97]. En effet, la distribution de clé d'un groupe forme une partie de la jonction d'un système à l'arbre du groupe. La jonction sécurisée implique la fournitutre de l'authentification, de l'intégrité et de la confidentialité

aux messages de jonction à CBT. Le contrôleur du groupe (Tree Core) délègue la distribution des clefs et la vérification des membres, joignant l'arbre, aux routeurs connectés à l'arbre.

L'inconvénient de cette approche est qu'ell edépend du protocole de routage. Ceci pose des problèmes lorsqu'elle est utilisée avec d' autres protocoles de routage. Autrement dit, elle est limitée à l'intra-domaine où il y a le protocole CBT.

4.5.2 LKH (Logical Key Hierarchy)

Ces approches proposent un compromis entre le coût temporel, l'espace de stockage et le nombre de message transmis, en utilisant un système hiérarchique de clés auxiliaires (nœuds intermédiaires logiques) pour faciliter la distribution de la clé du groupe. Le résultat est que l'espace de stockage nécessaire pour chaque membre et le nombre de transmissions exigés pour le renouvellement d'une clé sont logarithmiques par rapport à la taille du groupe. Nous pouvons citer comme exemple de ce type [Wallner 98, Wong 98] où les travaux de [Wallner 98] sont un cas particulier de [Wong 98]. En fait, ce dernier se base sur la notion de graphe de clés et de groupe sécurisé. Un groupe sécurisé est un triplet (U,K,R): U est l'ensemble des usagers, K l'ensemble des clés et R un sous-ensemble de U X R tel (u,k)$\in$ R $\Leftrightarrow$ l'usager u possède la clé k. Un graphe de clés est un graphe orienté acyclique avec deux types de nœuds: u-nœud représentant un usager et k-nœud représentant une clé. Un graphe spécifie un groupe sécurisé de la manière suivante:

- Chaque u de U correspond à u-nœud.
- Chaque k de K correspond à k-nœud.
- Pour chaque (u,k) de R il y a un chemin de u-nœud (lié à u) à k-nœud (lié à k).

Un graphe de clés avec un seul k-nœud dont aucun arc n'en sort est appelé un arbre. La figure 1 represente un graphe (arbre) de clé enraciné en K1234.

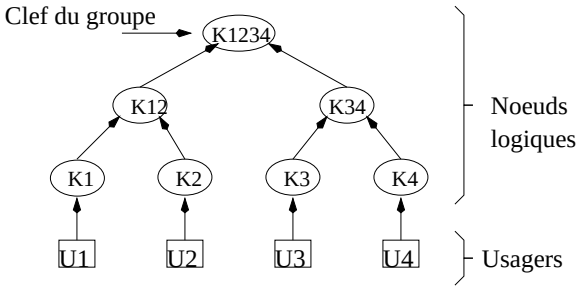

FIG. 1 – *Graphe de Clés ; U1,U2,U3,U4: u-noeuds(usagers) ; K1,K2,K3,K4,K12,K34,K1234: k-noeuds(clés) ; K1234 clé du groupe; U3 a les clés K3,K34,K1234*

Les feuilles sont les usagers et le k-nœud représentent la racine est la clé du groupe. Cet arbre est géré par le manager du groupe. Il distribue ces clés par le biais des tunnels

sécurisés de communication, de telle sorte que chaque usager ait les clés sur le chemin entre son u-nœud et la racine. L'ajout (la suppression) d'un membre exige le changement des clés existant sur le chemin liant le nœud ajouté (supprimé) et la racine, puis la distribution de ces clés aux membres concernés.

4.5.3 OFT (One-way Function Tree)

Le manager du groupe maintient un arbre binaire [McGrew 98, Balenson 99]. Une feuille représente un membre du groupe. Le manager attribue une clé à chaque membre qui sera la clé du nœud représentant le membre. Chaque nœud de OFT est associé à deux clés: clé de nœud k_x (dite clé non-aveugle) et clé aveugle $k_x{}' = g(k_x)$. La clé aveugle d'un nœud est calculée à partir de k_x en utilisant *One-way Function* g ; elle est aveugle dans le sens où un adversaire avec un peu de calcul peut apprendre $k_x{}'$, mais pas k_x. Le manager communique ces clés aux membres par le biais des tunnels de sécurité extérieurs. Les clefs des nœuds sont définies par la règle:

$$k_x = f(g(k_{gauche(x)}),g(k_{droit(x)}));$$

telque *gauche*(x) (*droit*(x)) est le fils *gauche* (*droit*) du nœud x. k_x est la clé de x. g est *one-way function* et f une fonction de mélange (e.g XOR). Une fois qu'un membre a sa propre clé et les clés non-aveugles des nœuds liés directement à son chemin à la racine, il peut calculer les clés sur son chemin vers la racine (voir figure 2).

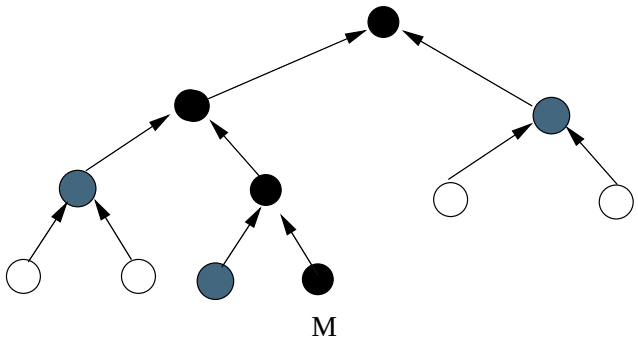

FIG. 2 – *Arbre d'un OFT: Le membre M connait les clés aveugles des nœuds noirs (y compris celle de la racine qui est la clé du groupe) et les clés non-aveulges des nœuds gris*

L'operation d'ajout ou du retrait d'un membre dépend de la communication d'une nouvelle clé aveugle à tous les membres concernés.

4.6 Analyse comparative

Malheureusement, pour assurer la sécurité à long terme contre les coalitions des membres suprimés, les approches de théorie d'information nécessitent un espace de stockage exponen-

tiel. Ainsi, les approches de Diffie-Hellman de groupe souffrent d'un nombre linéaire d'opérations de clés publiques qui sont très coûteuses. En général, pour les approches basées sur la théorie d'information, cryptographie à clé publique (*i.e.* Diffie-Hellmann de groupe), approches hybrides et SDKC, les besoins en espace de stockage, en calcul et en nombre de messages échangés croissent linéairement avec la taille (nombre de participants) du groupe pour les opérations d'ajout ou du retrait d'un participant. Tandis que pour les approches hiérarchiques, ces besoins croissent logarithmiquement.

De plus, les trois premiers catégories sont théoriques [Balenson 99] et la sécurité de certaines méthodes d'entre elles n'est pas vérifiée. Quant au SKDC et aux approches hiérarchiques, elles sont plus pratiques. Le reste de cette section sera consacré à analyser et à comparer SKDC et les deux approches hiérarchiques LKH et OFT.

Nous pouvons considérer SKDC la plus simple. Mais puisqu'elle ne résoud pas les deux problèmes d'extensibilté: **1 affect n** et **1 does not equal n**, elle ne convient qu'aux petits groupes de discussion.

Le tableau 1 récapitule le résultat de comparaison [Balenson 99] des besoins en calculs et transmissions à l'initialisation d'un groupe pour les trois approches SKDC, LKH et OFT : n représente la taille d'un groupe, K la taille de clé et h la hauteur de l'arbre binaire de LKH et OFT. C_E, C_r et C_g représentent respectivement le coût d'une seule évaluation d'une fonction de cryptage E, le coût de la génération aléatoire d'une clé par une source sécurisée et l'évaluation de one-way function g.

	SKDC	LKH	OFT
taille de trasmission	nK	2nK +h	2nK +h
calcul du manager	$n(C_E + C_r)$	$2n(C_E + C_r)$	$2n(C_E + C_g) + nC_r$
Calcul du membre	C_E	hC_E	hC_E

TAB. 1 – *Initialisation d'un groupe*

Nous constatons que la taille des messages diffusés pour LKH et OFT est le double de celle des messages diffusés pour SKDC. Ceci résulte du fait que chaque clé d'un arbre binaire à n feuilles, doit être diffusée aux membres. En conséquence, l'initialisation de SKDC est plus rapide et moins coûteuse que celle de deux autres.

Le tableau 2 résume la comparaison [Balenson 99] des besoins en calcul effectué par le manager et les membres, et la taille de transmissions du manager lors de chaque ajout et retrait d'un membre.

Dans le cas de SKDC, la taille de tranmissions du manager est nK, tandis que celle-ci est 2hK+h pour LKH et hK + h pour OFT. Donc OFT effectue moins de transmission. En général, LKH et OFT sont plus efficaces que SKDC.

Le tableau 3 compare [Balenson 99] les besoins en stockage pour les trois méthodes. Nous remarquons que SKDC nécessite un espace de stockage moins important que pour LKH et OFT.

	SKDC	LKH	OFT
taille de trasmission	nK	2hK +h	hK +h
calcul du manager	$n(C_E + C_r)$	$h(2C_E + C_r)$	$h(C_E + 2C_g) + C_r$
Calcul du membre	C_E	hC_E	$h(C_E + C_g)$

TAB. 2 – *ajout ou retrait d'un participant*

	SKDC	LKH	OFT
Stockage du manager	nK	2nK	2nK
Stockage d'un membre	2K	hK	hK

TAB. 3 – *Espace de staochage*

OFT et LKH résolvent le problème d'exensibilité **1 does not equal n** par le biais de la hiérarchie des clés.

En résumé, l'approche SKDC est plus efficace lors de l'initialisation d'un groupe que les approches hiérarchiques. De plus, elle exige un espace de stockage plus petit que les autres. En revanche, les approches hiérarchiques sont plus efficaces pour le dynamisme du groupe ; parce qu'elles distribuent l'effort du calcul de renouvellement de la clé du groupe sur différents participants du groupe.

Dans cette section, nous avons découvert et comparé les approches proposées pour la constuction et la distribution des clés servant à assurer des services de sécurité tels que la confidentialité, l'intégrité et à un type d'authentification qui est l'authentification de groupe. Nous présentons, dans la section suivante, des solutions proposées lors de l'authentification.

5 Authentification

Nous pouvons distinguer deux types d'authentification : l'authentification de groupe où l'émetteur est un membre du groupe et l'authentification individuelle où l'identité de l'émetteur est vérifiée indépendamment du groupe. En effet, l'authentification du groupe est assurée d'une manière implicite. Lorsqu'un récepteur réussit à déchiffrer les données, chiffrées avec la clé du groupe par un émetteur, il en déduit que l'émetteur possède la clé du groupe, *i.e.* est bien un membre du groupe.

Cependant, la clé partagée par les membres du groupe ne peut pas être utilisée pour différencier les différents émetteurs du groupe. En fait, la seule solution connue pour l'authentification individuelle est la signature à clés publiques. Mais, cela nécessite des surcharges sur les données lors de la génération de la signature.

Dans [Canetti 98b] est présentée une solution basée sur des mécanismes de clés partagées qui s'appellent MAC (Message Authentication Code) [Schneier 97]. Cette solution est plus

efficace (surtout dans le temps nécessaire pour générer la signature) que l'authentification à clés publiques. La solution part d'un schéma de base avec un seul émetteur puis elle propose des améliorations pour la rendre valable pour n émetteurs/récepteur en même temps.

Dans le schéma de base, l'émetteur gère un ensembe U de clés. Chaque récepteur R possède un sous-ensemble U_r clés tel que $U_r \subset U$. Les sous-ensembles U_r sont distribués de telles sorte que la probabilité qu'une coalition de récepteurs connaissant toutes les clés soit limitée. Un émetteur calcule pour chaque paquet les MACs correspondant aux clés qu'il possède et les attache au paquet émis. Chaque récepteur dans le groupe vérifie les MACs qui correspondent à ses clés. Une coalition corrompue de récepteurs ne peut pas authentifier un message et l'envoyer sans connaître toutes les clés du véritable récepteur ou casser le MAC.

La comparaison de performance entre ce schéma et celui de la signature à clés publiques revèle que le premier réduit le temps de calcul de l'émetteur et celui de vérification du récepteur. Par conséquent, il réduit la surcharge de communication. Plus les MACs sont efficaces plus le schéma à clés partagées est efficace.

Le schéma à clés partagées peut s'étendre à un schéma permettant à n'importe quel membre du groupe d'envoyer des données authentifiées multicasts. Un ensemble global de clés et chaque partie E connaît un sous-ensemble aléatoire U_e des clés. Quand un émetteur E envoie un message, il l'authentifie avec toutes les clés de U_e. Chaque récepteur R vérifie les MACs correspondant aux clés appartenant à l'intersection de U_e et U_r, *i.e.* $U_e \cap U_r$.

L'inconvénient de ce schéma est qu'il devient trop compliqué, même impossible à appliquer pour les grands groupes existant sur Internet. Sa difficulté s'explique par la gestion d'un grand nombre de clés distribuées de manière aléatoire aux les participants. Par contre, elle reste une bonne idée pour les très petits groupes.

Dans la suite, nous allons parler des travaux menés par l'IETF pour standardiser la sécurité d'IP multicat en se basant sur les standards de sécurité unicast.

6 Sécurité d'IP multicast

Face à la croissance permanente et à la commercialisation de l'Internet, le multicast est une solution efficace pour réduire l'utilisation de la bande passante, des ressources de l'émetteur et des ressources du réseau. Mais, assurer la sécurité des données multicast est beaucoup plus complexe que celle de données point-à-point. Récemment, plusieurs travaux [Canetti 99, Canetti 98a, Hardjono 99a, Harney 97a, Ballardie 96] de l'IETF ont abordé la sécurité du multicast sur Internet. Parmi ces travaux, [Canetti 99] propose une architecture de sécurité d'Internet multicast.

Cette architecture (figure 3) essaie de réutiliser les mécanismes d'IPsec dans la mesure du possible. Elle utilise AH [Atkinson 98a] et ESP [Atkinson 95] d'IPsec, implémentés dans le noyau du système opérationnel, pour authentifier et crypter les données multicast. Cette architecture sépare le plan du contrôle du plan des données. Le premier comprend les modules responsables de la gestion de l'adhésion et le contrôle d'accès au groupe. Quant au deuxième, il contient les modules qui sont responsables de la distribution des données multicasts et des opérations de chiffrement et d'authentification. Le module MIKE (Multicast Internet

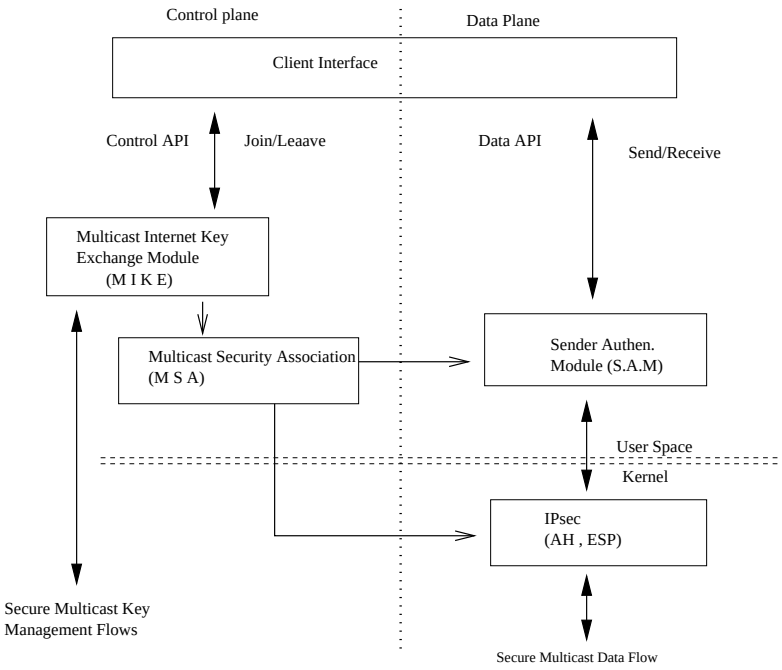

FIG. 3 – *Architecture d'IP multicast*

Key Exchange) inspiré de IKE[Harkins 98] est responsable de la gestion des clés et des associations de sécurité multicast.

La plupart des autres propostions se concentrent sur la gestion des clés multicasts. Dans le contexte de l'architecture précédente, ces propositions peuvent être incorporées dans le module MIKE. Ainsi [Hardjono 99a, Hardjono 99b] proposent de diviser le groupe multicast en sous-groupes distribués sur des régions. Ils introduisent le terme région pour promouvoir l'extensibilité en permettant à chaque région d'être définie à partir de protocoles et d'entités disponibles sur le plan d'infrastructure de réseau et d'être compatible avec les applications multicasts considerées. Ils définissent une solution extensible au problème de la gestion des clés d'un groupe dispersé sur l'Internet. L'inconvenient de cette solution est qu'elle impose un traitement supplémentaire sur les données multicasts échangées entre régions ; ce qui implique une diminution de la bande passant sur le réseau. BALLARDIE [Ballardie 96] propose également une solution au problème d'extensibilité de la distribution des clés multicasts. Cette solution se base sur le protocole CBT (Core Based Tree) multicast. La distribution des clés du groupe forme une partie du processus de la jonction d'un système à l'arbre du groupe. Elle exige des routeurs intermédiaires fiables existant sur l'arbre CBT et qui prendent en charge la distribution des clés du groupe. Le problème de cette solution est

qu'elle ne réagit pas lors de la supression d'un membre du groupe; il faut construire l'arbre à nouveau. De plus, elle n'est pas indépendante de protocole de routage.

Quant à l'approche GKMP [Harney 97a], elle est spécifiée pour travailler dans un environnement de multi-niveaux de sécurité. Elle permet à une entité, manager du groupe, de créer et de distribuer les clefs de groupe en coopérant avec les membres de groupe. Le manager du groupe contrôle l'accès au groupe en vérifiant les permissions des membres. La centralisation de la gestion du groupe est l'un des défauts de cette solution. Ainsi, le nombre de messages échangés lors de l'initialisation du groupe est important.

Tous ces travaux ne sont que des essais car la sécurisation de multicast sur Internet est très compliquée à cause des problèmes venant de l'extensibilité d'IP multicast [Pansiot 99]:

- Nombre et taille des groupes;
- Problème d'allocation d'adresses;
- Espace d'adressage limité (cas de IPv4);
- Contrôle du flux;
- Interaction entre protocoles de routage intra/inter domaine;
- Etats à mémoriser par les routeurs;
- Signalisation entre routeurs.

En conséquence, [Hardjono 99a, Hardjono 99b] est plus extensible que les autres travaux car il prend en compte la topologie d'Internet à l'échelle mondiale. Mais, il est loin d'être complet. De plus, il se base sur des protocoles de distribution de clé point-à-point pour la distribution des clés dans un groupe.

7 Conclusion

Dans cet article, Nous avons présenté un aperçu général sur l'état de l'art de la sécurité des communications de groupe. Nous avons vu que la problématique de la sécurité dans ce type de communication apparaît, pour les groupes dynamiques et étendus, sous forme de deux types de problèmes d'extensibilité: **1 affect n** et **1 does not equal n**.

Nous nous sommes concentrés sur les approches d'établissement des clés multicasts et de gestion de la sécurité multicast. Nous avons présenté et comparé différentes approches d'établissement de clés multicast. En effet, SKDC est la plus simple et la plus efficace mais elle ne résoud pas les problème d'extensibilté. Par contre, LKH et OFT sont plus efficaces pour le dynamisme du groupe et résolvent le deuxième type de problèmes. Quant aux approches hybrides, théorie d'information et Diffie-Hellmann de groupe, elles restent très théoriques.

Nous avons présenté également des approches du contrôle d'accès au groupe. Les travaux présentés par [Mittra 97, Hardjono 99a, Hardjono 99b] divisent le groupe en sous-groupes et résolvent donc le type **1 affect n**, mais ils sont moins efficaces que [Harney 97a, Wallner 98, Wong 98] pour les transmissions de communication de groupe.

Enfin, nous constatons qu'il n'existe pas de solution satisfaisante pour la sécurité multicast. Une telle solution devra fournir [Chaddoud 98]:

- un temps minimal de configuration de groupe ;
- un trafic aussi réduit que possible ;
- un groupe dynamique, *i.e.* retrait et ajout d'un membre possible à tout moment ;
- une indépendance des protocoles de toutage ;
- une confidentialité, intégrité et authentification des données ;
- une décentralisation de la gestion du groupe.

Références

[Atkinson 95] R. Atkinson. IP Encapsulating Security Payload (ESP), August 1995. Request For Comments rfc-1827: Network Working Group.

[Atkinson 98a] R. Atkinson. IP Authentication Header, August 1998. Request For Comments rfc-1826: Network Working Group.

[Atkinson 98b] R. Atkinson et S. Kent. Security Architecture for the Internet Protocol, November 1998. Request For Comments rfc-2401: Network Working Group.

[Balenson 99] D. Balenson, D. McGrew et A Sherman. Key Management for Large Dynamic Groups: One-way Function Trees and Amortized Initialization, February 1999. Intenet draft: draft-balenson-groupkeymgmt-oft-00.txt.

[Ballardie 96] T. Ballardie. Scalable Multicast Key Distribution, may 1996. Request For Comments rfc-1949: Network Working Group.

[Ballardie 97] A. Ballardie. Core Based Trees (CBT version 2) Multicast Routing, September 1997. Request For Comments rfc-2189: Network Working Group.

[Blundo 92] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro et M. Yung. *Perfectly-Secure Key Distribution for Dynamic Conferences.* Advances in Cryptology: proceedings of Crypto92,E. F. Brickell, Ed., LNCS 740, Springer-Verlag (1992), 471-486, 1992.

[Burmester 97] M. Burmester et Y. G. Desmedt. *Efficient and Secure Conference-Key Distribution.* Secure Protocole, M. Lomas, Ed. , LNCS 1189, Springer-Verlag, 119-130., 1997.

[Canetti 98a] R. Canetti et B. Pinkas. A Taxonomy of Multicast Security Issues, May 1998. Intenet draft: draft-canetti-secure-multicast-taxonomy-00.txt.

[Canetti 98b] R. Canetti, B. Pinkas, J. Garay, D. Micciiancio, M. Noar et G. Itkis. Multicast Security: A Taxonomy and Efficient Authentication. Rapport, IBM, April 1998.

[Canetti 99] R. Canetti, P. Cheng, D. Pendarakis, J. Rao, R. Rohatgi et D. Saha. An Architecture for Secure Internet Multicast, February 1999. Intenet draft: draft-irtf-smug-sec-mcast-arch-00.txt.

[Chaddoud 98] Ghassan Chaddoud. La sécurité dans IPv6 pour des applications multi-points. Stage de dea, LORIA, 98.

[Fiat 93] A. Fiat et M. Noar. Broadcast Encryption. Rapport, 1993.

[Floyd 95] S. Floyd, V. Jacobson, C.G. Liu, S. McCanne et L. Zhang. *A Reliable Multicast Framework for Light-weight Sessions and Application Level Framing.* pages 352–356. ACM-SIGCOMM'95, August 1995.

[Hardjono 99a] T. Hardjono, B. Cain et N Doraswamy. A Framework for Group Key Management for Multicast Security, August 1999. Intrenet draft: draft-ietf-ipsec-gkmframework-01.txt.

[Hardjono 99b] T. Hardjono, B. Cain et I Monga. Intra-Domain Group Key Management Protocol, August 1999. Internet draft: draft-ietf-ipsec-intragkm-00.txt.

[Harkins 98] D. Harkins et D. Carrel. The Internet Key Exchange (IKE), March 1998. RFC: <draft-ietf-ipsec-isakmp-oakley-07.txt>.

[Harney 97a] H. Harney et C. Mucknhirn. Group Key Management Protocol (GKMP) Architecture, July 1997. Request For Comments rfc-2094: Network Working Group.

[Harney 97b] H. Harney et C. Mucknhirn. Group Key Management Protocol (GKMP) Specification, July 1997. Request For Comments rfc-2093: Network Working Group.

[Maughan 98] D. Maughan, M. Schertler et M. Schneider. Internet Security Association and Key Management Protocol (ISAKMP), March 1998. Internet draft: <draft-ietf-ipsec-isakmp-09.txt>.

[McGrew 98] David A. McGrew et Alan T. SHerman. *Key Establishment in Large Dynamic Groups using One-way Function Trees.* TIS Labs at Network Associates, Inc. Gleenwood, Maryland, 1998.

[Mittra 97] S. Mittra. *Iolus: A Framework for Scalable Secure Multicasting.* ACM-SIGCOMM'97, septembre 1997.

[Monga 99] I. Monga et T. Hardjono. Group security association (gsa) deefinition for ip multicast, August 1999. Internet draft: draft-irtf-smug-gsadef-00.txt.

[Pansiot 99] J.J. Pansiot et A. Alloui. Routage multipoint inter-domaine, septembre 1999. Ecole d'été RHDM'99.

[Pusteri 99] T. Pusteri. Distance Vector Multicast Routing Protocol, February 1999. Internet draft: <draft-ietf-idmr-dvmrp-v3-08>.

[Schneier 97] B. Schneier. *Cryptographie Appliquée.* International Thomson Publishing, 1997. Traduction de L. Viennot.

[Steiner 96] M. Steiner, G. Tsudik et M. Wainder. *Deffie-Hellmen Key Distribution Extended to Group Communication.* 3rd ACM conference on Computer and Communication Security, New Delhi, India, 14-16March 1996.

[Wallner 98] D. Wallner, E. Harder et R Agee. Key Management for Multicast: Issues and Architecture, September 1998. Intenet draft: draft-wallner-key-arch-01.txt.

[Wong 98] C. Wong, M. Gouda et S. Lam. *Secure Group Communications using Key Graphs.* ACM-SIGCOMM'98, septembre 1998.

LORIA
Campus scientifique
BP 23
54506 VANDŒUVRE LÈS NANCY
http://www.loria.fr